UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Miscellaneous Case No. _____

WILLIAM ROSE, an individual,

Plaintiff,

v.

CELLULAR TOUCH WIRELESS, INC., a Florida corporation;

Defendant.

_____/

PLAINTIFF'S MOTION TO COMPEL COMPLIANCE WITH NON-PARTY SUBPOENA SERVED UPON KPMG, LLP

Plaintiff WILLIAM ROSE, an individual (hereinafter "Plaintiff"), by and through his undersigned counsel and pursuant to Federal Rules of Civil Procedure 7(b) and 45 and S.D. Fla. Local Rule 7.1, hereby submits this motion requesting that this Honorable Court enter an Order compelling compliance with the subpoena served upon non-party KPMG, LLP ("KPMG") and entering all appropriate relief in connection therewith, as set forth herein.

In support of his motion, Plaintiff states:

FACTUAL BACKGROUND AND PROCEDURAL HISTORY

THE LAWSUIT

1. On January 11, 2023, Plaintiff filed his Complaint for Damages and Equitable Relief in the matter styled William Rose v. Cellular Touch Wireless, Inc., United States District Court - Middle District of Florida - Case No. 2:23-cv-00022-JLB-KCD (the "Lawsuit") [MD Fla. DE 1]. *See*, **Exhibit "A"** hereto.

2. The Lawsuit is brought by Plaintiff, a Metro by T-Mobile subscriber who lost approximately Two Hundred Eighty Thousand Dollars ($280,000.00) worth of cryptocurrency in August 2021 in an under-recognized identity theft crime called "SIM swapping" or "SIM hijacking."

3. Defendant CELLULAR TOUCH WIRELESS, INC. ("Defendant") is an Exclusive Indirect Dealer who operates retail store locations in Florida under the brand of cellular telecommunications provider Metro by T-Mobile -- a discount service provider in the T-Mobile USA, Inc. ("T-Mobile") family of companies and the telecom provider through whom Plaintiff received his monthly cellphone service.

4. According to an August 27, 2021 press release issued by T-Mobile and its Chief Executive Officer Mike Sievert, "*On August 17th, we confirmed that T-Mobile's systems were subject to a criminal cyberattack that compromised data of millions of our customers, former customers, and prospective customers.*" *See*, **Exhibit "B"** hereto.

5. The August 2021 T-Mobile press release went on to state:

> ***Today I'm announcing that we have entered into long-term partnerships with the industry-leading cybersecurity experts at Mandiant****, and with consulting firm KPMG LLP.* ***We know we need additional expertise to take our cybersecurity efforts to the next level—and we've brought in the help.*** *These arrangements are part of a substantial multi-year investment to adopt best-in-class practices and transform our approach. This is all about assembling the firepower we need to improve our ability to fight back against criminals and building a future-forward strategy to protect T-Mobile and our customers.*
>
> *As I previously mentioned, Mandiant has been part of our forensic investigation since the start of the incident, and we are now expanding our relationship to draw on the expertise they've gained from the front lines of large-scale data breaches and use their scalable security solutions to become more resilient to future cyber threats. They will support us as we develop an immediate and longer-term strategic plan to mitigate and stabilize cybersecurity risks across our enterprise.*
>
> *Simultaneously,* ***we are partnering with consulting firm KPMG, a recognized global leader in cybersecurity consulting. KPMG's cybersecurity team will bring its deep expertise and interdisciplinary approach to perform a thorough review of all T-Mobile security policies and performance measurement. They will focus on controls to identify gaps and areas of improvement.*** *Mandiant and* ***KPMG will work side-by-side with our teams to map out definitive actions that will be designed to protect our customers and others from malicious activity now and into the future. I am confident in these partnerships and optimistic about the opportunity they present to help us come out of this terrible event in a much stronger place with improved security measures.***

(emphasis added).

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

6. Documents maintained by, *inter alia*, Defendant, T-Mobile, Metro by T-Mobile, and cybersecurity expert KPMG demonstrate that employees or employee credentials at a Defendant store location were used to effectuate the unauthorized SIM swap and account takeover imposed upon Plaintiff, which was vital in the scheme to steal Plaintiff's assets – a scheme that exploited certain internal cybersecurity flaws known to Metro by T-Mobile, T-Mobile, Defendant, and KPMG yet not adequately remedied and which exposed Plaintiff to the harm he suffered.

7. For example, when engaging KPMG in 2021 to thoroughly review all of T-Mobile's security policies and performance measurements to identify gaps and areas of improvement, T-Mobile gave KPMG consultants e-mail addresses using the "@t-mobile.com" domain and gave them accounts providing access to T-Mobile's Microsoft SharePoint platform to communicate with T-Mobile about the problems identified -- a decision designed to hide that information and frustrate discovery of those communications related to the T-Mobile security breaches and KPMG's proposed solutions thereto.

8. As a result of those reviews and communications between KPMG and T-Mobile, recommendations were presented to T-Mobile: (a) addressing some of the problems that persisted at the time Plaintiff's account was hacked, and (b) offering scalable security solutions for T-Mobile to become more resilient to future cyber threats – subjects that are unquestionably relevant to Plaintiff's claim in this matter and the cybersecurity flaws that led, in large part, to the harm addressed in his Complaint.

9. Plaintiff's Complaint makes the relevance of that information plainly clear. The following are but a few examples from the Complaint of why it is relevant:

> PARAGRAPH 28: SIM swaps are commonly executed by attackers who gain authorized or unauthorized access to a wireless provider's computer networks or who gain such access with the assistance of witting or unwitting individuals who had access to the telecommunications provider's networks.
>
> * * *

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

PARAGRAPH 52: Upon further information and belief, Defendant was aware that its security systems and internal software platform contained significant holes and weaknesses that permitted unchecked security bypasses and allowed unauthorized actors to enter the system and gain control over customer accounts and information; yet Defendant did not take adequate measures to address those holes and weaknesses.

* * *

PARAGRAPH 92: Defendant likewise knew that Plaintiff's Personal Information was vulnerable to hacks by thieves and other criminals because, *inter alia*, Metro by T-Mobile acknowledged such in its Privacy Policy, COBC, and CPNI Policy.

PARAGRAPH 93: Defendant thus knew of the substantial and foreseeable harms that could occur to Plaintiff if Defendant did not place adequate security on Plaintiff's Personal Information and did not follow its own security measures for Plaintiff's account.

* * *

PARAGRAPH 95: Plaintiff signed up for Metro by T-Mobile's wireless services and agreed to provide his Personal Information to Metro by T-Mobile with the understanding that Metro by T-Mobile and its agents would take appropriate measures to protect it. But Defendant -- acting as an authorized agent of Metro by T-Mobile -- did not protect Plaintiff's Personal Information and violated his trust.

PARAGRAPH 96: Defendant knew its security was inadequate.

* * *

PARAGRAPH 99: Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including CPI and CPNI, by failing to adopt, implement, and maintain adequate security measures to safeguard that information, including its duty under the FCA, the CPNI Rules, and its own Privacy Policy, COBC, and CPNI Policy.

PARAGRAPH 100: Defendant's failure to comply with federal and state requirements for security further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including CPI and CPNI.

PARAGRAPH 101: But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff, his Personal Information, including his CPI and CPNI, would not have been compromised, stolen, viewed, and used by unauthorized persons.

PARAGRAPH 102: Defendant's negligence was a direct and legal cause of the theft of Plaintiff's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of approximately $280,000.00 worth of cryptocurrency.

PARAGRAPH 103: The injury and harm suffered by Plaintiff was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including his CPI and CPNI.

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

10. Plaintiff needs to obtain and rely upon the documents created and reviewed by KPMG to support his claims, and to overcome Defendant's anticipated defenses, in the Lawsuit.

THE SUBPOENA

11. On May 23, 2023, Plaintiff propounded upon non-party KPMG a subpoena duces tecum in accordance with Fed.R.Civ.P. 45 (the "KPMG Subpoena"). *See*, **Exhibit "C"** hereto. The KPMG Subpoena calls for KPMG to produce certain documents in this jurisdiction.

12. The KPMG Subpoena was duly served upon KPMG on June 13, 2023. *See*, **Exhibit "D"** hereto.

13. On July 20, 2023, Plaintiff received from counsel for KPMG a set of formal Objections and Responses to the KPMG Subpoena. *See*, **Exhibit "E"** hereto.

14. Undersigned counsel and counsel for KPMG have participated in multiple Zoom videoconference sessions to address and narrow KPMG's Objections and Responses to the KPMG Subpoena. Notwithstanding undersigned counsel's good faith efforts, KPMG has not withdrawn any of its objections. Moreover, despite representing on multiple occasions that it would produce the documents in its possession that are responsive to the Subpoena, KPMG has not produced any of those documents.

15. For example, KPMG's counsel sent to undersigned counsel a letter dated October 6, 2023 in which KPMG represented it would produce to Plaintiff several documents, including the following:

> KPMG has conducted a reasonable search and is in the process of collecting and reviewing draft versions of the two reports and related documents synthesizing its control validation work for T-Mobile USA, Inc. ("T-Mobile"). This is also consistent with the agreement we reached during the August 16, 2023 meet and confer and further memorialized in our August 18, 2023 letter ("KPMG's August 18 Letter") to conduct additional reasonable searches for documents relating to KPMG's review of cybersecurity controls in response to Request Nos. 3 and 4 of the Subpoena.

* * *

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

> **Engagement Letter(s) between KPMG and T-Mobile:** KPMG will produce the engagement letter in connection with the controls validation engagement.
>
> * * *
>
> **Documents identifying KPMG agents working on the project to "evaluate T-Mobile's cyber controls":** KPMG will produce the requested information to the extent it is reflected on the draft controls validation reports discussed above.
>
> * * *
>
> **Final reports or draft reports or sketches:** As stated in KPMG's September 14 Letter and further discussed above, KPMG is working to collect and review draft versions of the two reports and related documents relating to its controls validation engagement with T-Mobile. KPMG will produce the most recent versions of these documents in its possession, custody, and control.

See, **Exhibit "F"** hereto (underlined emphasis added; bold type in original).

16. No production has been made by KPMG, though.

17. On October 20, 2023, KPMG (through its counsel) insisted that Plaintiff execute a Stipulated Confidentiality Agreement prepared by KPMG's counsel before KPMG would produce to Plaintiff any of the documents KPMG has that respond to the Subpoena.

18. On October 24, 2023, the undersigned law firm executed KPMG's proposed Stipulated Confidentiality Agreement and returned the document to KPMG's counsel, requesting KPMG's countersignature so the documents long-withheld by KPMG would finally be produced.

19. Although KPMG ultimately countersigned its own proposed Stipulated Confidentiality Agreement a month later (November 22, 2023), KPMG has refused to produce its responsive documents thereunder.

20. As of the date of this filing, KPMG's counsel has withdrawn from further discussions with undersigned counsel regarding the Subpoena.

KPMG IS WITHHOLDING RELEVANT DOCUMENTS AND INFORMATION

21. As noted above, KPMG possesses vital information relevant to this dispute that Plaintiff cannot obtain from any other source.

22. Notwithstanding undersigned counsel's good faith efforts spanning seven months to gain KPMG's compliance with the May 2023 Subpoena, KPMG has thus far failed to produce any such documents in response to the Subpoena.

23. Undersigned counsel has met several times with KPMG's counsel over the past seven months and has complied with KPMG's ever-increasing requirements to clear the path for KPMG's production of its responsive documents. Each time undersigned counsel has complied, though, KPMG has erected additional barriers and has moved the proverbial goalposts further and further away from any good faith compliance by KPMG with its obligation to respond to the Subpoena.

24. In light of the foregoing, Plaintiff requests that the Court overrule KPMG's objections and self-created obstacles and compel KPMG to produce all responsive documents in its possession, custody, or control without further delay.

DISCUSSION

"Parties may obtain discovery regarding any nonprivileged matter that is relevant to any...claim or defense and proportional to the needs of the case." Fed.R.Civ.P. 26(b)(1). The typical mechanism to obtain discovery from a nonparty is a subpoena. *See*, Fed.R.Civ.P. 45.

Under Rule 45, a non-party may be compelled by subpoena to produce documents and to permit an inspection of records. *See*, Fed.R.Civ.P. 45(d), (e). The scope of discovery provided for under Rule 26 similarly applies to discovery sought via a Rule 45 subpoena on a non-party. *See*, Fed.R.Civ.P. 45(a)(1).

To be relevant, evidence must have a "tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." Fed.R.Evid. 401. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. *Id.*

Information relevant to a party's claim or defense includes information that a party may use to support its denial or rebuttal of the claims or defenses of another party.

Here, the information sought through the KPMG Subpoena has substantial relevance to the claims and defenses of the parties in the Lawsuit. As Paragraph 9 above and its citations to Plaintiff's Complaint clearly demonstrates, the security measures undertaken by Defendant and T-Mobile to secure the customer service software and platform used by Defendant and T-Mobile -- measures that failed to comply with federal and state requirements and which contributed to Plaintiff's harm -- are undeniably relevant to matters that bear on, or reasonably could lead to other matters that could bear on, issues that are or may be in the case. T-Mobile itself has publicly stated that KPMG has conducted a forensic investigation and reviewed T-Mobile's security systems, and through that review KPMG has both obtained and generated documents that address some of the security flaws that are relevant to Plaintiff's claims. KPMG has admitted it has the documents; it just refuses to produce them. That refusal is unjustified, misplaced, and should be rejected by this Court.

While Plaintiff takes issue with the impropriety and lack of support to some of the objections stated in KPMG's formal written response to the Subpoena, Plaintiff reserves his right to address those matters with the Court as appropriate while keeping the focus of this motion on procuring from KPMG the relevant and responsive documents KPMG has admitted it has in its possession, custody, and control and had agreed to produce but now apparently needs to be compelled by the Court to make its production.

CONCLUSION

WHEREFORE, Plaintiff WILLIAM ROSE respectfully requests the Court enter an Order:

(a) compelling non-party KPMG, LLP ("KPMG") to comply with the Subpoena by producing to Plaintiff, within ten (10) days of the Court's Order, all documents KPMG has in its possession, custody, or control that respond to the Subpoena;

(b) granting such other relief as the Court deems just and appropriate.

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

CERTIFICATE OF COMPLIANCE WITH LOCAL RULE 7.1(a)(3)

Notwithstanding standard requirements that parties to litigation meet and confer with one another in a good faith effort to resolve by agreement the issues raised by a discovery motion before seeking judicial intervention on the issue, several federal courts "have dispensed with requiring a party and non-party to meet and confer prior to filing a motion under Rule 45." *Housemaster SPV LLC v. Burke*, Civil Action No. 21-13411 (MAS), 2022 WL 17904254, at *7 (D. N.J. Dec. 23, 2022); *Clift v. City of Burlington*, No. 2:12-CV-214, 2013 WL 12347197, at *2 (D. Vt. Aug. 26, 2013) ("A non-party filing a Rule 45 motion therefore does not need to meet and confer prior with the counsel of the party serving the subpoena"); *Jackson v. AFSCME Local 196*, 246 F.R.D. 410, 413 (D. Conn. 2007) (Rule 45 does not require that the parties (and non-parties) meet and confer prior to the filing of a motion); *Travelers Indem. Co. v. Metropolitan Life Ins. Co.*, 228 F.R.D. 111 (D. Conn. 2005).

Nevertheless, Plaintiff's counsel has conferred in good faith with counsel for KPMG to narrow the issues in dispute in this matter. However, those efforts have not produced any meaningful resolution of any part of this motion.

Respectfully submitted,

SILVER MILLER
4450 NW 126th Avenue - Suite 101
Coral Springs, Florida 33065
Telephone: (954) 516-6000

By: */s/ David C. Silver*
DAVID C. SILVER
Florida Bar No. 572764
E-mail: DSilver@SilverMillerLaw.com
JASON S. MILLER
Florida Bar No. 072206
E-mail: JMiller@SilverMillerLaw.com

Counsel for Plaintiff William Rose

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that the foregoing document was electronically filed this 26th day of December 2023 using the CM/ECF filing system, which will send electronic notice of filing to all registered counsel and parties in this action.

I FURTHER CERTIFY that a true and correct copy of the foregoing document was sent on this 26th day of December 2023 via electronic mail to: **MARGARET GEMBALA NELSON, ESQ. and ELYSIA A. LAMPERT, ESQ.**, FOLEY & LARDNER LLP, *Counsel for KPMG LLP*, 321 North Clark Street - Suite 3000, Chicago, IL 60654-4762, E-mail: MNelson@foley.com, ELampert@foley.com.

/s/ David C. Silver
DAVID C. SILVER